SCOTT EDELSBERG
CA Bar No. 330990
scott@edelsberglaw.com
EDELSBERG LAW, P.A.
1925 Century Park E #1700
Los Angeles, CA 90067
Telephone: 305.975.3320

Attorney for Plaintiff and Proposed Class

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

TREVOR HOLDEN, individually, and on behalf of all others similarly situated,

Plaintiff,

vs.

CALIBRATED HEALTHCARE, LLC

Defendant.

Case No. _____

CLASS ACTION COMPLAINT

1. Negligence
2. Negligence *per se*
3. Breach of Fiduciary Duty
4. Breach of Implied Contract
5. Invasion of Privacy
6. Unjust Enrichment
7. Declaratory Judgement

DEMAND FOR JURY TRIAL

Plaintiff, Trevor Holden ("Plaintiff"), brings this Class Action Complaint ("Complaint") against Defendant Calibrated Healthcare, LLC, ("Calibrated" or "Defendant"), as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions, and upon information and belief and his counsels' investigation as to all other matters, as follows:

INTRODUCTION

1. Plaintiff seeks monetary damages and injunctive and declaratory relief arising from Defendant's failure to safeguard the Personally Identifiable Information[1] ("PII") and Protected Health Information ("PHI") (together, "Private Information") of its customers, which resulted in unauthorized access to its information systems between February 25 and February 26, 2024, and the compromised and unauthorized disclosure of that Private Information, causing widespread injury and damages to Plaintiff and the proposed Class (defined below) members.

2. Defendant, Calibrated Healthcare, LLC is a healthcare management company that provides administrative and clinical healthcare services to entities across the United States.[2]

3. As explained in detail herein, on or around February 26, 2024, Calibrated detected unusual activity in its computer systems and ultimately determined that an unauthorized third party accessed its network and obtained certain files from its systems between February 25 and February 26, 2024 ("Data Breach").[3]

4. As a result of the Data Breach, which Defendant failed to prevent, the Private Information of Defendant's customers, including Plaintiff and the proposed Class members, were

---

[1] The Federal Trade Commission ("FTC") defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8). To be clear, according to Defendant, not every type of information included in that definition was compromised in the subject data breach.

[2] The "Notice of Data Breach." Attached hereto as ***Exhibit A***.

[3] *Id.*

stolen, including their name, date of birth, medical information, health insurance information, and health benefit plan number.[4]

5. Defendant's investigation concluded that the Private Information compromised in the Data Breach included Plaintiff's and other individuals' information (together, "Customers").

6. Defendant's failure to safeguard Customers' highly sensitive Private Information as exposed and unauthorizedly disclosed in the Data Breach violates its common law duty, California law, and Defendant's implied contract with its Customers to safeguard their Private Information.

7. Plaintiff and Class members now face a lifetime risk of identity theft due to the nature of the information lost, which they cannot change, and which cannot be made private again.

8. Defendant's harmful conduct has injured Plaintiff and Class members in multiple ways, including: (i) the lost or diminished value of their Private Information; (ii) costs associated with the prevention, detection, and recovery from identity theft, tax fraud, and other unauthorized use of their data; (iii) lost opportunity costs to mitigate the Data Breach's consequences, including lost time; and (iv) emotional distress associated with the loss of control over their highly sensitive Private Information.

9. Defendant's failure to protect Customers' Private Information has harmed and will continue to harm Defendant's Customers, causing Plaintiff to seek relief on a class wide basis.

10. On behalf of himself and the Class preliminarily defined below, Plaintiff brings causes of action against Defendant for negligence, negligence *per se*, breach of fiduciary duty,

---

[4] *Id.*

breach of implied contract, invasion of privacy, and unjust enrichment seeking an award of monetary damages, resulting from Defendant's failure to adequately protect their highly sensitive Private Information.

PARTIES

11. Plaintiff is, and at all times mentioned herein was, an individual resident and citizen of the State of Florida.

12. Plaintiff sought and received healthcare services from a healthcare provider. As a condition of receiving services, Plaintiff was required to provide the healthcare provider with his Private Information. The healthcare provider subsequently provided this Private Information to Defendant as a condition of receiving administrative and clinical healthcare services.

13. Based on representations made by Defendant, Plaintiff believed Defendant implemented and maintained reasonable security to protect his Private Information.

14. If Plaintiff had known that Defendant would not adequately protect his Private Information, he would not have allowed Defendant to maintain this sensitive Private Information.

15. Defendant Calibrated Healthcare, LLC is a Limited Liability Company organized under the laws of California with its headquarters and principal place of business at 3633 Inland Empire Blvd., Suite 301, Ontario, CA 91764.

JURISDICTION AND VENUE

16. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members is over 100, and at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, including Plaintiff. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

17. This Court has personal jurisdiction over Defendant Calibrated Healthcare, LLC because its principal place of business is in California, and it does a significant amount of business in California.

18. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Calibrated Healthcare, LLC has its principal place of business located in this District, and a substantial part of the events giving rise to this action occurred in this District.

FACTUAL BACKGROUND

Defendant Calibrated's Business

19. Calibrated Healthcare, LLC is a California-headquartered administrative and clinical healthcare service provider serving entities across the United States.[5]

20. Plaintiff and Class members sought services from a healthcare provider and provided their Private Information to these healthcare providers. This Private Information was then provided to Defendant as a condition of the healthcare providers receiving administrative and clinical healthcare services.

21. To obtain healthcare services, Customers, including Plaintiff and Class members, were required to provide sensitive and confidential Private Information, including their names, dates of birth, health records, insurance information, and other sensitive information, that would be held by Calibrated in its computer systems.

22. The information held by Calibrated at the time of the Data Breach included the unencrypted Private Information of Plaintiff and Class members.

[5] https://calibratedhealthcare.com (last accessed September 11, 2024)

23. Upon information and belief, Calibrated made promises and representations to its Customers that the Private Information collected would be kept safe and confidential, the privacy of that information would be maintained, and Calibrated would delete any sensitive information after it was no longer required to maintain it.

24. Plaintiff and Class members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

25. Plaintiff and Class members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiff and Class members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

26. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class members from involuntary disclosure to third parties. Defendant has a legal duty to keep Customers' Private Information safe and confidential.

27. Defendant had obligations under the FTC Act, HIPAA, contract, industry standards, and representations made to Plaintiff and Class members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

28. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class members' Private Information. Without the required submission of Private Information, Defendant could not perform the services it provides.

29. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class members' Private Information from disclosure.

The Data Breach

30. On or about September 6, 2024, Defendant began notifying Customers of the Data Breach, informing them by an untitled letter("Notice")[6]:

> **What Happened?** On February 26, 2024, Calibrated identified suspicious activity related to certain systems within its computer network. In response, Calibrated promptly took the systems offline and began an investigation. The investigation determined that certain portions of Calibrated's network were accessed between February 25 and February 26, 2024 and, during that timeframe, certain files were likely copied without authorization. As a result of that determination, Calibrated initiated a comprehensive review of the data to determine what type of information was present and to whom it relates. This review was recently completed and identified information relating to some of our customers. We began notifying our customers on May 1, 2024, and worked with them to notify potentially impacted individuals, including you.
>
> **What Information Was Involved?** Our investigation determined that the following information was present in the reviewed files: name; date of birth; medical information; health insurance information and health benefit plan number.
>
> **What We Are Doing.** In response to this incident, we dedicated significant resources to confirming the security of our network, conducting a comprehensive investigation and completing a detailed review of the relevant files. We then notified our potentially affected customers and worked with them to provide notice to potentially impacted individuals as quickly as possible. As part of our ongoing commitment to the security of information in our care, we are also reviewing our existing policies and procedures and enhancing our existing security tools.

[6] Exhibit A.

31. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiff and Class members, such as encrypting the information or deleting it when it is no longer needed, causing the exposure of Private Information.

32. The attacker accessed and acquired files in Defendant's computer systems containing unencrypted Private Information of Plaintiff and Class members, including name, date of birth, medical information, health insurance information and health benefit plan number. Plaintiff's and Class members' Private Information was accessed and stolen in the Data Breach.

33. Plaintiff further believes his Private Information, and that of Class members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

The Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' Private Information.

34. As a condition to obtain services from healthcare providers, Plaintiff and Class members were required to give their sensitive and confidential Private Information to the healthcare providers. Subsequently, the healthcare providers gave Plaintiff's and Class members' Private Information to Calibrated in order to receive its administrative and clinical healthcare services.

35. Calibrated retains and stores this information and derives a substantial economic benefit from the Private Information that it collects. But for the collection of Plaintiff's and Class members' Private Information, Calibrated would be unable to perform its services.

36. By obtaining, collecting, and storing the Private Information of Plaintiff and Class members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the Private Information from disclosure.

37. Plaintiff and Class members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendant to keep their Private Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

38. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiff and Class members.

39. Upon information and belief, Defendant made promises to Plaintiff and Class members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information.

40. Defendant's negligence in safeguarding the Private Information of Plaintiff and Class members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

Defendant Knew or Should Have Known of the Risk of a Cyber Attack Because Healthcare Entities in Possession of Private Information Are Particularly Suspectable to Cyber Attacks.

41. Data thieves regularly target entities in the healthcare industry like Defendant due to the highly sensitive information that they maintain. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

42. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting healthcare entities like Defendant that collect and store Private Information and other sensitive information, preceding the date of the Data Breach.

43. In light of recent high profile data breaches at other industry-leading companies, including, *e.g.*, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the Private Information that it collected and maintained would be targeted by cybercriminals.

44. For example, of the 1,862 recorded data breaches in 2021, 330 of them, or 17.7%, were in the medical or healthcare industry.[7]

45. The 330 breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[8]

46. Entities in custody of Private Information and/or medical information reported the largest number of data breaches among all measured sectors in 2022, with the highest rate of exposure per breach.[9] Indeed, when compromised, healthcare related data is among the most

---

[7] 2021 Data Breach Annual Report (ITRC, Jan. 2022), https://notified.idtheftcenter.org/s/, at 6.

[8] *Id*.

[9] *See* Identity Theft Resource Center, *2022 Annual Data Breach Report*, https://www.idtheftcenter.org/publication/2022-data-breach-report/ (last accessed September 11, 2024).

sensitive and personally consequential. A report focusing on healthcare breaches found the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that victims were often forced to pay out of pocket costs for healthcare they did not receive in order to restore coverage.[10] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. 40 percent of the patients were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals, and detrimentally impact the economy as a whole.[11]

47. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class members from being compromised.

48. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to over one million individuals' detailed Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

49. The injuries to Plaintiff and Class members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class members.

---

[10] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed September 11, 2024).

[11] *See id.*

50. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiff and Class members are long lasting and severe. Once Private Information is stolen fraudulent use of that information and damage to victims may continue for years.

51. As a healthcare entity in possession of its Patients' Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiff and Class members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class members because of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

Defendant Fails to Comply with FTC Guidelines

52. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

53. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[12]

[12] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed September 11, 2024).

54. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[13]

55. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

56. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

57. These FTC enforcement actions include actions against healthcare entities, like Defendant. *See, e.g.*, *In the Matter of LabMD, Inc., a corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

[13] *Id.*

58. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

59. Defendant failed to properly implement basic data security practices.

60. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Patients' Private Information or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

61. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the Private Information of its Patients; Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

Defendant Fails to Comply with HIPAA Guidelines.

62. Defendant is a covered businesses under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

63. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[14] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

64. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

65. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

66. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

67. "Electronic protected health information" is "individually identifiable health information . . . that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

68. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

[14] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

d. Ensure compliance by its workforce.

69. HIPAA also requires Defendant to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant are required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

70. HIPAA and HITECH also obligate Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic PHI that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

71. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

72. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of PHI in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

73. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in

the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[15] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.[16]

Defendant Owed Plaintiff and Class Members a Duty to Safeguard their Private Information.

74. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class members.

[15] https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last accessed September 11, 2024)

[16] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (last accessed September 11, 2024).

75. Defendant owed a duty to Plaintiff and Class members to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees and others who accessed Private Information within its computer systems on how to adequately protect Private Information.

76. Defendant owed a duty to Plaintiff and Class members to implement processes that would detect a compromise of Private Information in a timely manner.

77. Defendant owed a duty to Plaintiff and Class members to act upon data security warnings and alerts in a timely fashion.

78. Defendant owed a duty to Plaintiff and Class members to disclose in a timely and accurate manner when and how the Data Breach occurred.

79. Defendant owed a duty of care to Plaintiff and Class members because they were foreseeable and probable victims of any inadequate data security practices.

The Data Breach Increases Plaintiff's and Class Members' Risk of Identity Theft.

80. The unencrypted Private Information of Plaintiff and Class members will end up (if it has not already ended up) for sale on the dark web, as that is the *modus operandi* of hackers.

81. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class members.

82. Simply put, unauthorized individuals can easily access the Private Information of Plaintiff and Class members because of the Data Breach.

83. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information.

Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

84. Plaintiff's and Class members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and Class members and to profit from their misfortune.

Loss of Time to Mitigate the Risk of Identity Theft and Fraud

85. As a result of the recognized risk of identity theft, when a data breach occurs and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm.

86. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class members must monitor their financial accounts for many years to mitigate the risk of identity theft.

87. Plaintiff and Class members have spent, and will spend additional time in the future, on a variety of prudent actions, such as changing passwords and resecuring their own computer systems.

88. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in

which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[17]

89. Plaintiff's mitigation efforts are also consistent with the steps the FTC recommends data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[18]

90. And for those Class members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

Diminution of Value of Private Information.

91. Private Information is valuable property.[19] Its value is axiomatic, considering the value of Big Data in corporate America and that the consequences of cyber thefts include heavy

---

[17] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf (last accessed September 11, 2024).

[18] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last accessed September 11, 2024).

[19] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," at 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last accessed September 11, 2024) ("GAO Report").

prison sentences. Even this obvious risk-to-reward analysis illustrates, beyond doubt, that Private Information has considerable market value.

92. The Private Information stolen in the Data Breach is significantly more valuable than the loss of, say, credit card information in a large retailer data breach. Victims affected by those retailer breaches could avoid much of the potential future harm by simply cancelling credit or debit cards and obtaining replacements. The information stolen in the Data Breach is difficult, if not impossible, to change.

93. This kind of data, as one would expect, demands a much higher price on the dark web. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[20]

94. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[21]

---

[20] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hackpersonal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed September 11, 2024).

[21] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private Information") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

95. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[22] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[23,24] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[25]

96. As a result of the Data Breach, Plaintiff's and Class members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

97. The fraudulent activity resulting from the Data Breach may not come to light for years.

98. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class members are

---

[22] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last accessed September 11, 2024).

[23] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last accessed September 11, 2024).

[24] https://datacoup.com/ (last accessed September 11, 2024).

[25] https://www.thepennyhoarder.com/make-money/nielsen-panel/#:~:text=Sign%20up%20to%20join%20the,software%20installed%20on%20your%20computer (last accessed September 11, 2024).

incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

99. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to millions of individuals' detailed Private Information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

100. The injuries to Plaintiff and Class members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class members.

The Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary.

101. Given the type of targeted attack in this case, the sophisticated criminal activity, the volume of data compromised in this Data Breach, and the sensitive type of Private Information involved in this Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

102. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Private Information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

103. Consequently, Plaintiff and Class members are at an increased risk of fraud and identity theft for many years into the future.

104. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class member. This is a reasonable and necessary cost to monitor and protect Class members from the risk of identity theft resulting from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class members would not need to bear, but for Defendant's failure to safeguard their Private Information.

Loss of the Benefit of the Bargain

105. Furthermore, Defendant's poor data security deprived Plaintiff and Class members of the benefit of their bargain. When agreeing directly or indirectly to pay Defendant for the provision of its healthcare services, Plaintiff and other reasonable consumers understood and expected that they were, in part, paying for the service and necessary data security to protect the Private Information when, in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

Plaintiff's Experience

106. Plaintiff sought services from a healthcare provider that uses Calibrated for administrative and clinical healthcare services. To obtain these services, he was required to provide his Private Information to the healthcare provider.

107. Defendant provides administrative and clinical healthcare services to the healthcare provider, and in order to obtain these services, the healthcare provider was required to provide Plaintiff's Private Information to Defendant.

108. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff's Private Information in its system.

109. Plaintiff is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

110. Plaintiff learned of the data breach after reviewing the Notice of Data Breach. According to the Notice, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties. The Private Information comprised some combination of his name, date of birth, medical information, health insurance information, and health benefit plan number.

111. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including checking his bills and accounts to make sure they were correct. Plaintiff has spent significant time dealing with the Data Breach, valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

112. As a result of the Data Breach, Plaintiff fears for his personal financial security and uncertainty over what medical information was revealed in the Data Breach. He is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

113. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

114. As a result of the Data Breach, Plaintiff is presently at risk and will continue to be at increased risk of identity theft and fraud for years to come.

115. Plaintiff has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

116. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3), on behalf of a class defined as:

> All individuals whose Private Information was accessed and/or acquired by an unauthorized party in the Data Breach, including all who were sent a notice of the Data Breach.

117. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

118. Plaintiff reserves the right to amend the definition of the Class or add a Class or Subclass if further information and discovery indicate that the definition of the Class should be narrowed, expanded, or otherwise modified.

119. **Numerosity**: The Class members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, it is likely that hundreds, if not thousands, of individuals had their Private Information compromised in this Data Breach. The Class is apparently identifiable within Defendant's records.

120. Common questions of law and fact exist as to all Class members and predominate over any questions affecting solely individual Class members. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, are the following:

a. Whether and to what extent Defendant has a duty to protect the Private Information of Plaintiff and Class members;

b. Whether Defendant has respective duties not to disclose the Private Information of Plaintiff and Class members to unauthorized third parties;

c. Whether Defendant has respective duties not to use the Private Information of Plaintiff and Class members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class members;

e. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

f. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

g. Whether Plaintiff and Class members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct; and

h. Whether Plaintiff and Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

121. **Typicality**: Plaintiff's claims are typical of those of the other Class members because Plaintiff, like every other Class member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

122. This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

123. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of Class members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Class members. Plaintiff seeks no relief that is antagonistic or adverse to Class members and the infringement of the rights and the damages he has suffered are typical of other Class members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

124. **Superiority**: Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that millions of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class members, who could not individually

afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

125. The nature of this action and the nature of laws available to Plaintiff and Class members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

126. Adequate notice can be given to Class members directly using information maintained in Defendant's records.

127. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

a. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

b. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

c. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

d. Whether Defendant's failure to institute adequate protective security measures amounted to breach of an implied contract;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to HIPAA and FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

CAUSES OF ACTION

COUNT I
Negligence
(On behalf of Plaintiff and the Classes)

128. Plaintiff hereby repeats and realleges paragraphs 1 through 127 of this Complaint and incorporates them by reference herein.

129. Healthcare providers require their Patients, including Plaintiff and Class members, to submit non-public Private Information in the ordinary course of providing healthcare services.

130. Defendant requires healthcare providers, to submit Customers' non-public Private Information in the ordinary course of providing administrative and clinical healthcare services.

131. Defendant gathered and stored the Private Information of Plaintiff and Class members as part of its business of soliciting its services to its healthcare providers, which solicitations and services affect commerce.

132. Plaintiff and Class members directly or indirectly entrusted Defendant with their Private Information with the understanding that Defendant would safeguard their information.

133. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class members could and would suffer if the Private Information were wrongfully disclosed.

134. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

135. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

136. Defendant owed a duty of care to Plaintiff and Class members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

137. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Patients. That special relationship arose because Plaintiff and Class members directly or indirectly entrusted Defendant with their

confidential Private Information, which was a necessary part of seeking services from health providers who used Calibrated for administrative and clinical healthcare services.

138. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

139. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

140. Defendant breached its duties, thus was negligent, by failing to use reasonable measures to protect Class members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, (a) failing to adopt, implement, and maintain adequate security measures to safeguard Class members' Private Information; (b) failing to adequately monitor the security of their networks and systems; and (c) allowing unauthorized access to Class members' Private Information.

141. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly considering Defendant's inadequate security practices.

142. It was foreseeable that Defendant's failure to use reasonable measures to protect Class members' Private Information would result in injury to Class members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

143. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class members could and would suffer if the Private Information were wrongfully disclosed.

144. Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and Class members, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

145. It was therefore foreseeable that the failure to adequately safeguard Class members' Private Information would result in one or more types of injuries to Class members.

146. Plaintiff and Class members had no ability to protect their Private Information that was in, and likely remains in, Defendant's possession.

147. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

148. Defendant's duty extended to protecting Plaintiff and Class members from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

149. Defendant has admitted that the Private Information of Plaintiff and Class members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

150. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class members, the Private Information of Plaintiff and Class members would not have been compromised.

151. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and Class members and the harm, or risk of imminent harm, suffered by Plaintiff and Class members. The Private Information of Plaintiff and Class members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

152. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of their Private Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

153. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

154. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Defendant's possession and is subject to further unauthorized

disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

155. Plaintiff and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

156. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class members.

COUNT II
Negligence *Per Se*
(On behalf of Plaintiff and the Classes)

157. Plaintiff hereby repeats and realleges paragraphs 1 through 127 of this Complaint and incorporates them by reference herein.

158. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

159. Pursuant to HIPAA, 42 U.S.C. § 1302d *et seq*., Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class members' Private Information.

160. Pursuant to HIPAA, Defendant had a duty to render the electronic Private Information they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." *See* definition of encryption at 45 C.F.R. § 164.304.

161. Defendant breached its duties to Plaintiff and Class members under the FTC Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

162. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se.*

163. The injuries to Plaintiff and Class members resulting from the Data Breach were directly and indirectly caused by Defendant's violation of the statutes described herein.

164. Plaintiff and Class members were within the class of persons the Federal Trade Commission Act and HIPAA were intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statues were intended to guard against.

165. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class members, Plaintiff and Class members would not have been injured.

166. The injuries and harms suffered by Plaintiff and Class members were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties and that Defendant's breach would cause Plaintiff and Class members to experience the foreseeable harms associated with the exposure of their Private Information.

167. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class members have suffered injuries and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT III
Breach of Fiduciary Duty
(On behalf of Plaintiff and the Classes)

168. Plaintiff hereby repeats and realleges paragraphs 1 through 127 of this Complaint and incorporates them by reference herein.

169. Plaintiff and the other Class members sought services from a healthcare provider that uses Calibrated for administrative and clinical healthcare services. Plaintiff and the other Class members directly or indirectly provided Defendant their Private Information believing that Defendant would protect that information. Plaintiff and the other Class members would not have provided this information had they known it would not be adequately protected. Defendant's acceptance and storage of Plaintiff's and the other Class members' Private Information created a fiduciary relationship between Defendant on the one hand, and Plaintiff and the other Class members, on the other hand. In light of this relationship, Defendant must act primarily for the benefit of its customers, which includes safeguarding and protecting Plaintiff's and the other Class members' Private Information.

170. Due to the nature of the relationship between Defendant and Plaintiff and the other Class members, Plaintiff and the other Class members were entirely reliant upon Defendant to ensure that their Private Information was adequately protected. Plaintiff and the other Class members had no way of verifying or influencing the nature and extent of Defendant's or their vendors' data security policies and practices, and Defendant was in an exclusive position to guard against the Data Breach.

171. Defendant has a fiduciary duty to act for the benefit of Plaintiff and the other Class members upon matters within the scope of their relationship. It breached that duty by failing to

comply with the data security guidelines set forth by HIPPA, and otherwise failing to safeguard Plaintiff's and the other Class members' Private Information that it collected.

172. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and the other Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their Private Information which remains in Defendant's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the Private Information compromised as a result of the Data breach; (vii) loss of potential value of their Private Information; (viii) overpayment for the services that were received without adequate data security.

COUNT IV
Breach of Implied Contract
(On behalf of Plaintiff and the Classes)

173. Plaintiff hereby repeats and realleges paragraphs 1 through 127 of this Complaint and incorporates them by reference herein.

174. Healthcare providers offered to provide healthcare services in exchange for payment and the production of Plaintiff's and Class Members' Private Information.

175. Defendant offered to provide administrative and clinical healthcare services to healthcare providers in exchange for payment, and Plaintiff's and the Class Members' Private Information.

176. In turn, Defendant impliedly promised to protect Plaintiff's and Class members' Private Information through adequate data security measures.

177. Plaintiff and the Class members accepted Defendant's offer by providing Private Information to their health providers, which was subsequently provided to Defendant in exchange for receiving Defendant's services, and then by paying for and receiving the same.

178. Plaintiff and Class members would not have entrusted their Private Information to Defendant but for the above-described agreement with Defendant.

179. Defendant materially breached its agreement(s) with Plaintiff and Class members by failing to safeguard such Private Information, violating industry standards necessarily incorporated in the agreement.

180. Plaintiff and Class members have performed under the relevant agreements, or such performance was waived by the conduct of Defendant.

181. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose on each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract along with its form.

182. Defendant's conduct as alleged herein also violated the implied covenant of good faith and fair dealing inherent in every contract.

183. The losses and damages Plaintiff and Class members sustained as described herein were the direct and proximate result of Defendant's breach of the implied contracts with them,

including breach of the implied covenant of good faith and fair dealing.

COUNT V
Invasion of Privacy
(On behalf of Plaintiff and the Class)

184. Plaintiff repeats and realleges paragraphs 1 through 127 of this Complaint and incorporate them by reference herein.

185. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

186. Defendant owed a duty to its current and former customers, including Plaintiff and the Class, to keep this information confidential.

187. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff and Class members' Private Information is highly offensive to a reasonable person.

188. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class directly or indirectly disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

189. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

190. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

191. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

192. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

193. As a proximate result of Defendant's acts and omissions, the private and sensitive Private Information of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages (as detailed *supra*).

194. And, on information and belief, Plaintiff's Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

195. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their Private Information is still maintained by Defendant with their inadequate cybersecurity system and policies.

196. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the Private Information of Plaintiff and the Class.

197. In addition to injunctive relief, Plaintiff, on behalf of himself and the other Class members, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

COUNT VI
Unjust Enrichment
(On behalf of Plaintiff and the Class)

198. Plaintiff repeats and realleges paragraphs 1 through 127 of this Complaint and incorporates them by reference herein.

199. This claim is pleaded in the alternative to the breach of implied contract claim.

200. Plaintiff and Class members (or their third-party agents) conferred a benefit upon Defendant. After all, Defendant benefitted from using their Private Information to provide services and/or receiving payment.

201. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class members (or their third-party agents).

202. Plaintiff and Class members (or their third-party agents) reasonably understood that Defendant would use adequate cybersecurity measures to protect the Private Information that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

203. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class members' Private Information.

204. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security measures. Plaintiff and Class members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

205. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and Class members' Private Information and/or payment because Defendant failed to adequately protect their Private Information.

206. Plaintiff and Class members have no adequate remedy at law.

207. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiff and Class members—all unlawful or inequitable proceeds that it received because of its misconduct.

COUNT VII
Declaratory Judgment
(*On Behalf of Plaintiff and the Class*)

208. Plaintiff repeats and realleges paragraphs 1 through 127 of this Complaint and incorporates them by reference herein.

209. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

210. In the fallout of the Data Breach, an actual controversy has arisen about Defendant's various duties to use reasonable data security. On information and belief, Plaintiff alleges that Defendant's actions were—and *still* are—inadequate and unreasonable. And Plaintiff and Class members continue to suffer injury from the ongoing threat of fraud and identity theft.

211. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;

b. Defendant has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. Defendant breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and

d. Defendant breaches of its duties caused—and continues to cause—injuries to Plaintiff and Class members.

212. The Court should also issue corresponding injunctive relief requiring Defendant to use adequate security consistent with industry standards to protect the data entrusted to it.

213. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendant experiences a second data breach.

214. And if a second breach occurs, Plaintiff and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiff's and Class members' injuries.

215. If an injunction is not issued, the resulting hardship to Plaintiff and Class members far exceeds the minimal hardship that Defendant could experience if an injunction is issued.

216. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiff, Class members, and the public at large.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class members, requests judgment against Defendant and that the Court grants the following:

A. For an order certifying the Class, as defined herein, and appointing Plaintiff and his Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws.

iii. requiring Defendant to delete, destroy, and purge the Private Information of Plaintiff and Class members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class members;

iv. requiring Defendant to implement and maintain a comprehensive information security program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class members;

v. prohibiting Defendant from maintaining the Private Information of Plaintiff and Class members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and security checks;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor

Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential Private Information to third parties, as well as the steps affected individuals must take to protect themselves; and

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct an attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment.

D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined by a jury at trial;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury of all issues so triable.

Dated: September 12, 2024.

Respectfully submitted,

By: *Scott Edelsberg*

Scott Edelsberg
CA Bar No. 330990
scott@edelsberglaw.com
EDELSBERG LAW, P.A.
1925 Century Park E #1700
Los Angeles, CA 90067
Telephone: 305.975.3320

Attorneys for Plaintiff and the Putative Class

EXHIBIT A

Calibrated Healthcare

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

11 1 3637 **********AUTO**ALL FOR AADC 331
Trevor Holden
[redacted]

September 6, 2024

Dear Trevor Holden:

Calibrated Healthcare, LLC ("Calibrated") provides administrative and clinical healthcare services to entities across the United States. We are writing to notify you of a data incident that may impact your information that we received in connection with the services we provide to NeueHealth.

What Happened? On February 26, 2024, Calibrated identified suspicious activity related to certain systems within its computer network. In response, Calibrated promptly took the systems offline and began an investigation. The investigation determined that certain portions of Calibrated's network were accessed between February 25 and February 26, 2024 and, during that timeframe, certain files were likely copied without authorization. As a result of that determination, Calibrated initiated a comprehensive review of the data to determine what type of information was present and to whom it relates. This review was recently completed and identified information relating to some of our customers. We began notifying our customers on May 1, 2024, and worked with them to notify potentially impacted individuals, including you.

What Information Was Involved? Our investigation determined that the following information was present in the reviewed files: name; date of birth;medical information;health insurance information and health benefit plan number.

What We Are Doing. In response to this incident, we dedicated significant resources to confirming the security of our network, conducting a comprehensive investigation and completing a detailed review of the relevant files. We then notified our potentially affected customers and worked with them to provide notice to potentially impacted individuals as quickly as possible. As part of our ongoing commitment to the security of information in our care, we are also reviewing our existing policies and procedures and enhancing our existing security tools.

As an added precaution, we are offering you 12 months of credit monitoring and identity protection services, through Equifax, at no cost to you. If you wish to activate these services, you may follow the instructions included in the *Steps You Can Take to Help Protect Personal Information* section on the next page of this letter. Please note you must enroll in these services directly, as we are unable to do so on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Again, additional information and resources may be found in the *Steps You Can Take to Help Protect Personal Information* section on the next page of this letter.